Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/EP04/053469

International filing date: 14 December 2004 (14.12.2004)

Document type: Certified copy of priority document

Document details: Country/Office: FR
Number: 03/15078
Filing date: 19 December 2003 (19.12.2003)

Date of receipt at the International Bureau: 23 May 2005 (23.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

PCT/EP2005/053469

R E P U B L I Q U E F R A N Ç A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

EPO - DG 1

10. 05. 2005

(76)

BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 31 MARS 2005

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint-Petersbourg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr

ETABLISSEMENT PUBLIC NATIONAL CREE PAR LA LOI N° 51-444 DU 19 AVRIL 1951

1er depot

INPI
INSTITUT NATIONAL DE LA PROPRIÉTÉ INDUSTRIELLE
26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

cerfa N° 11354*03

REQUÊTE EN DÉLIVRANCE
page 1/2

BR1

Cet imprimé est à remplir lisiblement à l'encre noire DB 540 @ W / 210502

Réservé à l'INPI

REMISE DES PIÈCES
DATE 19 DEC 2003
LIEU 75 INPI PARIS 34 SP
N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0315078
DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 19.12.2003.

Vos références pour ce dossier *(facultatif)* 017097 JPB/JPG/SM - GEM1525

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET BALLOT
Conseils en Propriété Industrielle
122, rue Edouard Vaillant
92593 LEVALLOIS PERRET CEDEX
Tél. 01.49.64.61.00 - Fax 01.49.64.61.20

Confirmation d'un dépôt par télécopie ☐ N° attribué par l'INPI à la télécopie

2 NATURE DE LA DEMANDE — **Cochez l'une des 4 cases suivantes**

Demande de brevet	☒	
Demande de certificat d'utilité	☐	
Demande divisionnaire	☐	
Demande de brevet initiale	N°	Date
ou demande de certificat d'utilité initiale	N°	Date
Transformation d'une demande de brevet européen *Demande de brevet initiale*	☐ N°	Date

3 TITRE DE L'INVENTION (200 caractères ou espaces maximum)
TELEPHONE PORTABLE ET PROCEDE ASSOCIE DE SECURISATION DE SON IDENTIFIANT.

4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE

Pays ou organisation — Date — N°
Pays ou organisation — Date — N°
Pays ou organisation — Date — N°
☐ **S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»**

5 DEMANDEUR (Cochez l'une des 2 cases) ☒ **Personne morale** ☐ **Personne physique**

Nom ou dénomination sociale		GEMPLUS
Prénoms		
Forme juridique		Société Anonyme
N° SIREN		3 4 9 7 1 1 2 0 0
Code APE-NAF		3 2 1 B
Domicile ou siège	Rue	Avenue du Pic de Bertagne - Parc d'activités de Gemenos
	Code postal et ville	1 3 4 2 0 GEMENOS
	Pays	FRANCE
Nationalité		FRANCAISE
N° de téléphone *(facultatif)*		N° de télécopie *(facultatif)*
Adresse électronique *(facultatif)*		

☐ **S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»**

Remplir impérativement la 2ème page

1er dépôt

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

REQUÊTE EN DÉLIVRANCE
page 2/2

BR2

Réservé à l'INPI

REMISE DES PIÈCES
DATE 19 DEC 2003
LIEU 75 INPI PARIS 34 SP

N° D'ENREGISTREMENT NATIONAL ATTRIBUÉ PAR L'INPI 0315078

DB 540 W / 210502

6 MANDATAIRE *(s'il y a lieu)*		
Nom		BENTZ
Prénom		Jean-Paul
Cabinet ou Société		CABINET BALLOT
N °de pouvoir permanent et/ou de lien contractuel		
Adresse	Rue	122, rue Edouard Vaillant
	Code postal et ville	9 2 5 9 3 LEVALLOIS-PERRET CEDEX
	Pays	
N° de téléphone *(facultatif)*		01 49 64 61 00
N° de télécopie *(facultatif)*		01 49 64 61 20
Adresse électronique *(facultatif)*		
7 INVENTEUR (S)		**Les inventeurs sont nécessairement des personnes physiques**
Les demandeurs et les inventeurs sont les mêmes personnes		☐ Oui ☒ Non : **Dans ce cas remplir le formulaire de Désignation d'inventeur(s)**
8 RAPPORT DE RECHERCHE		**Uniquement pour une demande de brevet (y compris division et transformation)**
Établissement immédiat ou établissement différé		☒ ☐
Paiement échelonné de la redevance *(en deux versements)*		**Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt** ☐ Oui ☐ Non
9 RÉDUCTION DU TAUX DES REDEVANCES		**Uniquement pour les personnes physiques** ☐ Requise pour la première fois pour cette invention *(joindre un avis de non-imposition)* ☐ Obtenue antérieurement à ce dépôt pour cette invention *(joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence)* : **AG**
10 SÉQUENCES DE NUCLEOTIDES ET/OU D'ACIDES AMINÉS		☐ Cochez la case si la description contient une liste de séquences
Le support électronique de données est joint		☐
La déclaration de conformité de la liste de séquences sur support papier avec le support électronique de données est jointe		☐
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		

11 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(Nom et qualité du signataire)
Levallois-Perret, le 18 décembre 2003

BENTZ Jean-Paul - CPI N° 99-0308

VISA DE LA PRÉFECTURE OU DE L'INPI

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire. Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

TELEPHONE PORTABLE ET PROCEDE ASSOCIE DE SECURISATION DE SON IDENTIFIANT

La présente invention porte sur les combinés de téléphonie mobile, et plus particulièrement sur les techniques visant à réduire les possibilités de réutilisation d'un combiné volé.

Le vol de combinés de téléphonie portable est devenu un véritable problème de société. Les vols avec violence dans les lieux publics ont ainsi massivement augmenté ces dernières années du fait des vols de tels combinés. On peut par exemple estimer que le nombre de téléphones portables volés en France durant l'année 2001 a été supérieur à 150 000. Pour combattre ces vols, les autorités françaises obligent dorénavant les opérateurs de téléphonie mobile à placer un identifiant des combinés volés sur une liste noire. Chaque combiné mobile présente une identification unique appelée IMEI (pour International Mobile Equipment Identity en langue anglaise) qui est transmise au réseau utilisé pour la communication. L'IMEI d'un combiné déclaré volé est ainsi placée dans une liste noire, qui est déjà opérationnelle en France. Lorsqu'un combiné inscrit dans la liste tente de communiquer, ses communications peuvent être bloquées.

Cependant, l'IMEI est actuellement stockée sur une mémoire flash et mal sécurisée. En effet, des logiciels permettent de modifier l'IMEI d'un combiné et sont disponibles en masse sur internet. Ainsi, comme cela a été reconnu par la Commission Européenne, la mise en

place de listes noires de combinés volés peut être contournée relativement aisément.

Une recommandation technique de l'ETSI propose de rendre l'IMEI inchangeable après le processus de fabrication du combiné. Cette recommandation a notamment été mise en œuvre en inscrivant l'IMEI dans une PROM, afin qu'elle ne puisse pas physiquement être modifiée.

Cette technique de sécurisation présente des inconvénients. En effet, l'IMEI est lue par le système d'exploitation du combiné. L'utilisation de systèmes d'exploitation frauduleux permet ainsi de modifier l'IMEI de façon logicielle afin de fournir une IMEI modifiée au réseau.

L'invention vise à résoudre ces inconvénients. L'invention a ainsi pour objet un combiné de téléphonie mobile comprenant :

-un support de stockage sécurisé contre les accès frauduleux, stockant l'IMEI du combiné ;

-un connecteur d'un module électronique sécurisé associé à un opérateur;

-un système d'exploitation du combiné, commandant l'authentification du support de stockage de l'IMEI par un module électronique sécurisé connecté au connecteur afin d'établir un canal de communication sécurisé entre le support de stockage et le module, et commandant la transmission de l'IMEI sur le canal sécurisé vers le module électronique sécurisé.

Selon une variante, le système d'exploitation commande la transmission de l'IMEI à un opérateur de

téléphonie mobile par l'intermédiaire d'un canal sécurisé OTA.

Selon une autre variante, le combiné comprend un module électronique sécurisé associé à l'opérateur connecté dans le connecteur. Selon encore une variante, le module électronique sécurisé est une carte UICC.

On peut alors prévoir que le système d'exploitation commande l'authentification du module sécurisé par le support de stockage.

Selon une variante, le module électronique sécurisé et le support de stockage stockent des clés de cryptage adaptées pour sécuriser le canal de communication sécurisé.

Selon une autre variante, le module sécurisé bloque l'utilisation du combiné lors de la détection d'une IMEI falsifiée.

L'invention porte également sur un procédé de sécurisation de l'IMEI d'un combiné de téléphonie mobile, comprenant les étapes :

-d'authentification d'un support de stockage sécurisé du combiné mémorisant son IMEI, par un module électronique sécurisé associé à l'opérateur et inséré dans un connecteur du combiné, afin d'établir un canal sécurisé entre le support de stockage et le module sécurisé;

-de transmission de l'IMEI depuis le support de stockage jusqu'au module sécurisé par l'intermédiaire du canal sécurisé.

Selon une variante, le module sécurisé transmet en outre l'IMEI à un opérateur de téléphonie mobile par l'intermédiaire d'un canal sécurisé OTA.

Selon encore une variante, l'opérateur compare l'IMEI à une liste noire de combinés volés, et bloque les communications du combiné lorsque le combiné appartient à la liste noire.

Selon une autre variante, le module sécurisé bloque l'utilisation du combiné lors de la détection d'une IMEI falsifiée.

D'autres particularités et avantages de l'invention apparaîtront clairement à la lecture de la description faite à titre d'exemple non limitatif et en regard des dessins annexés sur lesquels :

-la figure 1 représente des éléments mis en œuvre selon une variante de l'invention ;

-la figure 2 représente un diagramme illustrant les échanges et étapes réalisés par des éléments selon une variante de l'invention .

L'invention propose d'utiliser un canal sécurisé afin de réaliser une authentification d'un support de stockage (sécurisé contre les accès frauduleux et mémorisant l'IMEI) par un module électronique sécurisé associé à l'opérateur et connecté dans le combiné mobile. Un tel module électronique sécurisé se présente typiquement sous la forme d'une carte UICC (pour Universal Integrated Circuit Card en langue anglaise) par exemple au format d'une carte SIM. L'IMEI n'est transmise sur le canal sécurisé que lorsque le support de stockage de l'IMEI a été authentifié.

La figure 1 illustre ainsi un combiné de téléphonie mobile 1 selon l'invention. Le combiné 1 comprend un

support de stockage 2 sécurisé contre les accès frauduleux. Ce support de stockage 2 stocke l'IMEI 21 du combiné 1. Le combiné 1 comprend en outre un connecteur 3 pour un module électronique sécurisé tel qu'une carte UICC 31. Un canal de communication sécurisé 6 est établi entre le module électronique sécurisé 31 connecté dans le connecteur 3 et le support de stockage sécurisé 2. Le canal de communication sécurisé 6 signifie qu'au moins le module sécurisé authentifie le support de stockage 2 par tout moyen approprié et garantit l'intégrité et la confidentialité de toutes les données échangées. Un système d'exploitation 4 du combiné, commande l'authentification du support de stockage 2 de l'IMEI 21 par le module sécurisé 31 connecté dans le connecteur (identifié par l'étape 101 à la figure 2), et commande la transmission de l'IMEI sur le canal sécurisé 6 vers ce module sécurisé 31 (identifié par l'étape 102 à la figure 2).

L'IMEI est ainsi sécurisée contre les modifications dynamiques lors de sa transmission sur le canal de communication 6. On peut donc considérer que l'IMEI reçue par le module 31 est authentifiée car elle provient du support de stockage authentifié 2 et a été transmise par l'intermédiaire du canal de communication sécurisé 6.

Bien entendu, si l'authentification du support de stockage 2 de l'IMEI par le module électronique sécurisé 31 signale une erreur, ce module électronique

31 peut prendre toute mesure adaptée pour signaler cette erreur ou empêcher l'utilisation du combiné.

On peut ainsi bloquer le combiné sans avoir recours à une communication avec le réseau de l'opérateur. L'opérateur peut notamment éviter d'avoir à gérer les clés ou les certificats associés à un combiné. Un tel blocage est donc plus facile à mettre en œuvre. Un tel blocage du téléphone peut également être réalisé sans nécessiter de modifications des réseaux des opérateurs : les infrastructures et protocoles du réseau existant peuvent ainsi être conservés.

Le support de stockage 2 sécurisé contre les accès frauduleux peut être d'un type connu, par exemple une PROM. L'intégrité statique de l'information qui y est inscrite est ainsi assurée.

Afin de sécuriser le canal 6 et de réaliser toute authentification voulue entre le support de stockage 2 et le module 31, le support 2 et/ou le module peuvent stocker des clés de cryptage adaptées au type de cryptage ou d'authentification souhaités. Des types de cryptage ou d'authentification utilisables sont connus en soi. On peut notamment prévoir d'utiliser des clés de session ou des clés statiques.

L'intégrité de l'IMEI peut être protégée par un calcul cryptographique qui serait transmis sur le canal sécurisé 6 au module sécurisé 31.

Le système d'exploitation 4 peut être mémorisé dans une mémoire ROM et exécuté par un microcontrôleur. Le

système d'exploitation 4 établira de préférence un canal sécurisé entre le support 2 et le module sécurisé 31 au moment de l'initialisation du combiné de téléphonie, ou en préalable à un appel.

Le système d'exploitation 4 peut être configuré pour que le module sécurisé 31 authentifie le combiné et vérifie l'intégrité des données qui lui sont transmises. On peut également prévoir que le module sécurisé 31 soit authentifié par le support sécurisé 2 du mobile 1 et vérifie également l'intégrité des données qui lui sont transmises.

On peut également prévoir des moyens de calcul cryptographiques intégrés dans le module sécurisé 31.

L'utilisation des listes noires doit malgré tout être poursuivie pour prendre des mesures de blocage. L'IMEI peut notamment être transmise du module sécurisé vers le réseau de l'opérateur, éventuellement en utilisant un canal sécurisé entre le module sécurisé 31 et l'opérateur ou afin de comparer l'IMEI authentifiée à une liste noire et éventuellement obtenir une commande de blocage du combiné de la part du réseau. Dans l'exemple de la figure 2, l'IMEI est transmise à un serveur 7 à l'étape 103. Le serveur établit si cet IMEI est présente dans sa liste noire. A l'étape 104, le serveur transmet au combiné une indication de la présence ou non de l'IMEI dans la liste. Une indication de présence d'une IMEI dans la liste peut correspondre à une commande de blocage du combiné par le serveur. Le serveur peut bien entendu prendre toute autre mesure adéquate pour perturber l'utilisateur frauduleux. Le

serveur peut notamment déconnecter le combiné du réseau de communication de l'opérateur ou commander au module sécurisé de cesser la génération de clés pour le combiné.

Plusieurs modes de transmission de l'IMEI peuvent être envisagés entre le module sécurisé et le réseau de l'opérateur.

Cette transmission peut notamment être effectuée par l'intermédiaire du réseau de communication de l'opérateur, destiné à transmettre les communications entre utilisateurs. Dans l'exemple de la figure 1, la transmission est effectuée entre le combiné et un opérateur 5 d'un réseau de communication.

La transmission s'effectuera plutôt par l'intermédiaire d'un canal sécurisé, afin d'accroître le niveau de sécurité de la transmission. On peut notamment utiliser le canal sécurisé OTA initialement destiné à transmettre des SMS sécurisés et notamment utilisé pour le transfert d'applets, vers le module sécurisé.

REVENDICATIONS

1. Combiné de téléphonie mobile (1), caractérisé en ce qu'il comprend :
-un support de stockage (2) sécurisé contre les accès frauduleux, stockant l'identification IMEI (21) du combiné ;
-un connecteur (3) d'un module électronique sécurisé (31) associé à un opérateur;
-un système d'exploitation (4) du combiné (1), commandant l'authentification du support de stockage (2) de l'IMEI par un module électronique sécurisé connecté au connecteur afin d'établir un canal de communication sécurisé (6) entre le support de stockage et le module, et commandant la transmission de l'IMEI sur le canal sécurisé vers le module électronique sécurisé.

2. Combiné de téléphonie mobile (1) selon la revendication 1, caractérisé en ce que le système d'exploitation (4) commande la transmission de l'IMEI à un opérateur de téléphonie mobile (5) par l'intermédiaire d'un canal sécurisé OTA.

3. Combiné selon l'une quelconque des revendications précédentes, caractérisé en ce qu'il comprend un module électronique (31)

sécurisé associé à l'opérateur connecté dans le connecteur.

4. Combiné selon la revendication 3, caractérisé en ce que le module électronique sécurisé est une carte UICC.

5. Combiné selon la revendication 3 ou 4, caractérisé en ce que le système d'exploitation commande l'authentification du module sécurisé par le support de stockage.

6. Combiné selon la revendication 5, caractérisé en ce que le module électronique sécurisé et le support de stockage stockent des clés de cryptage (22) adaptées pour sécuriser le canal de communication sécurisé (6).

7. Combiné selon l'une quelconque des revendications 3 à 6, caractérisé en ce que le module sécurisé (31) bloque l'utilisation du combiné lors de la détection d'une IMEI falsifiée.

8. Procédé de sécurisation de l'identification IMEI d'un combiné de téléphonie mobile (1), comprenant les étapes ;

-d'authentification d'un support de stockage sécurisé du combiné mémorisant son IMEI (21), par un module électronique sécurisé (31) associé à l'opérateur et

inséré dans un connecteur (3) du combiné, afin d'établir un canal sécurisé entre le support de stockage et le module sécurisé;

-de transmission de l'IMEI (21) depuis le support de stockage jusqu'au module sécurisé par l'intermédiaire du canal sécurisé.

9. Procédé selon la revendication 8, caractérisé en ce que le module sécurisé (31) transmet en outre l'IMEI à un opérateur de téléphonie mobile par l'intermédiaire d'un canal sécurisé OTA.

10. Procédé selon la revendication 9, caractérisé en ce que l'opérateur compare l'IMEI à une liste noire (7) de combinés volés, et bloque les communications du combiné lorsque le combiné appartient à la liste noire.

11. Procédé selon l'une quelconque des revendications 8 à 10, caractérisé en ce que le module sécurisé bloque l'utilisation du combiné lors de la détection d'une IMEI falsifiée.

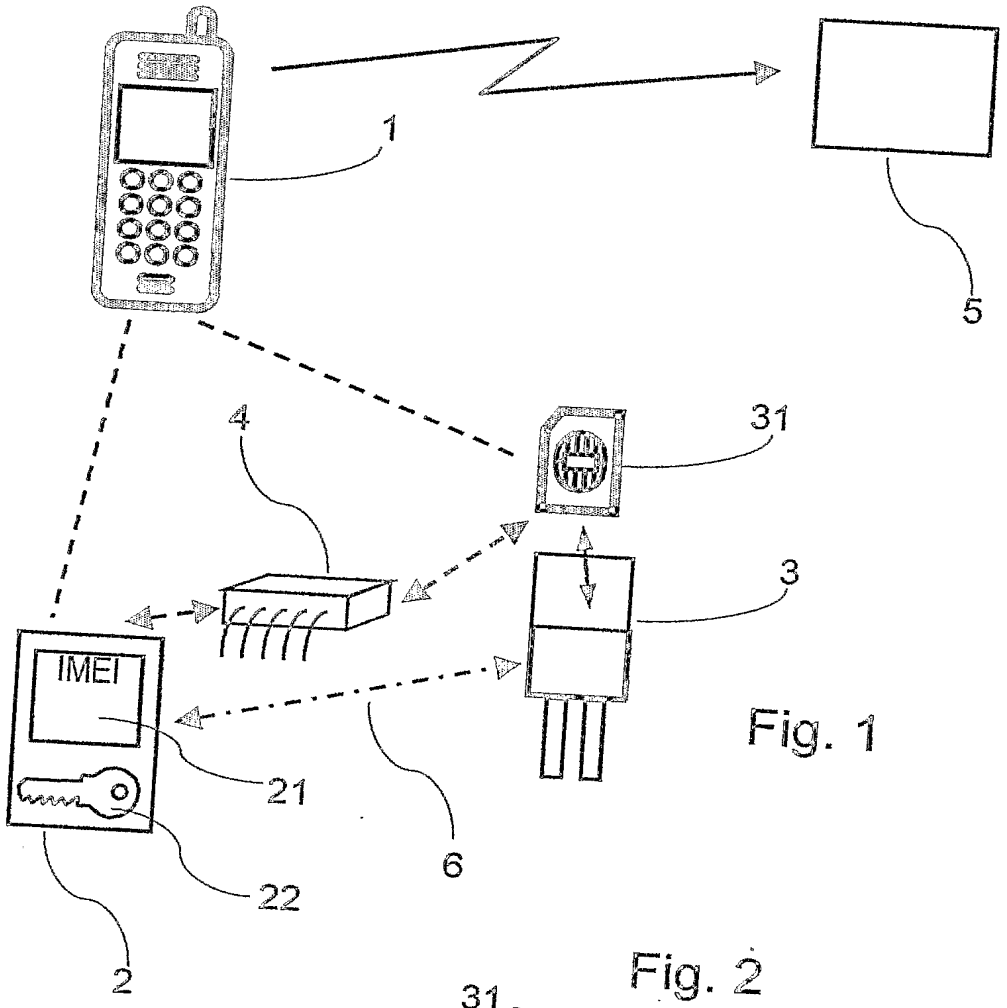
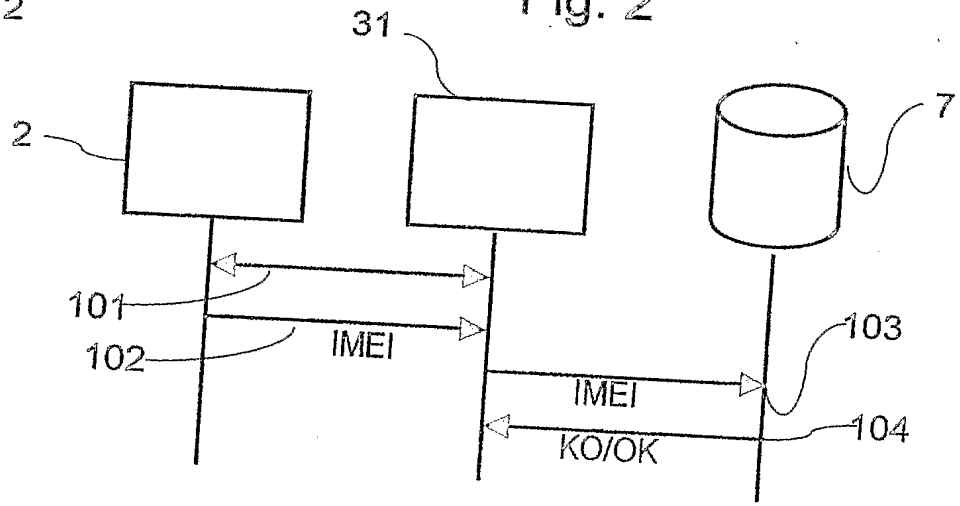


Fig. 1

Fig. 2



reçue le 02/02/04

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION
CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI

gemplus
N° 11235*03

DÉSIGNATION D'INVENTEUR(S) Page N° 1../1..

INV

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)

Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 @ W / 270601

Vos références pour ce dossier *(facultatif)*	017097 JPB/JPG/SM - GEM1525
N° D'ENREGISTREMENT NATIONAL	

TITRE DE L'INVENTION (200 caractères ou espaces maximum)

TELEPHONE PORTABLE ET PROCEDE ASSOCIE DE SECURISATION DE SON IDENTIFIANT.

LE(S) DEMANDEUR(S) :

GEMPLUS
Avenue du Pic de Bertagne
Parc d'activités de Gemenos
13420 GEMENOS
FRANCE

DESIGNE(NT) EN TANT QU'INVENTEUR(S) :

1 Nom		BOURSIER
Prénoms		Carine
Adresse	Rue	38, chemin de St Michel
	Code postal et ville	13400 AUBAGNE
Société d'appartenance *(facultatif)*		
2 Nom		GIRARD
Prénoms		Pierre
Adresse	Rue	942, chemin du Tourtaret
	Code postal et ville	13112 LA DESTROUSSE
Société d'appartenance *(facultatif)*		
3 Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance *(facultatif)*		

S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.

DATE ET SIGNATURE(S)
DU (DES) DEMANDEUR(S)
OU DU MANDATAIRE
(Nom et qualité du signataire)

Levallois-Perret, le 18 décembre 2003
BENTZ Jean-Paul
Mandataire N° 99-0308
Cabinet BALLOT